Direct Loan Central Database /
Direct Loan Servicing System (DLCD / DLSS)
Corrective Action Plan,
September 2000

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Security Life Cycle Planning	There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.		Ensure that (as appropriate) privacy and security in the information life cycle are addressed in DLCD/DLSS life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
2	Rules of Behavior	There was no evidence that the Rules of Behavior were documented.		Document rules of behavior for DLCD/DLSS. Ensure managers and users are trained to understand them.		
3	Authorize Processing	There was no evidence that DLCD/DLSS had been certified and accredited. Although DLCD/DLSS has not sought certification, this report could serve as the basis for a system certification/ authority to operate.		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal DLCD/DLSS certification test under NIST guidance (FIPS 102).		
4	System Interconnection/ Information Sharing	There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.		Ensure all DLCD/DLSS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.		
5	Personnel Security	Management of security clearance processing needed improvement (e.g., "…require any personnel not cleared to submit the required paperwork…", "..inform personnel, particularly program management, of the results of clearance processing…").		Implement ED personnel security guidance. See the Personnel Security section for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
6	Security Awareness and Training	More in-depth training needed to be provided to additional personnel.		Provide security training for the DLCD/DLSS SSO; once trained, the DLCD/DLSS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.		
7	Documentation	Disaster Recovery Plan (DRP) needed to be updated to reflect changes. The Security Plan needed to be updated based upon a recent revision of OMB Circular A-130.		Develop a NIST-compliant (Special Pub 800-18) security plan for DLCD/DLSS. See the Recommendations section for additional details.		
8	Central Security Focus/ Assigned Responsibility			Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness, and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.		
9	Physical and Environmental Protection	Security enhancements were needed (e.g., visitors needed positive identification, establish a sign-in log, etc.).		When developing/updating the DLCD/DLSS security plan, ensure the controls noted above are fully addressed.		
10	Application Software Maintenance Controls	There was no evidence of controls for the maintenance of the application.		Examine ED guidance relating to system life cycle planning. Ensure that DLCD/DLSS CM processes and procedures are consistent with that guidance, and that the DLCD/DLSS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
11	Data Integrity / Validation Controls	There was no evidence of controls for assuring the integrity and validity of the data.		Ensure DLCD/DLSS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.		
12	Public Access Controls	There was no evidence documenting whether or not public access was allowed to DLCD/DLSS.		Document and implement within one year DLCD/DLSS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.		
13	Audit Trails	There was no evidence to indicate that the audit trails were being reviewed by appropriate staff.		Ensure DLCD/DLSS audit results are being used effectively to help DLCD/DLSS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.		
14	Applicable Laws and Regulations	DLCD/DLSS is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.		N/A		
15	System Environment	There was no evidence of a technical description of the system.		See the recommendation for General Description/ Purpose above.		